Technical Cybersecurity Defenses

G-Free

Eliminates unaligned branching

- Remember, x86 is unaligned, allows for EIP to point to any location
- If all branching can only be from aligned instructions, majority of ROP calls are invalid

Checks function calls

- Appends a validation block to function calls

Return address protection

- Uses an XOR canary

Stronger ASLR

ASLR RANDOMIZES SOME NUMBER OF BITS

- 64-bit systems currently randomize ~40 bits
  - Can't brute force without discovery
- 32-bit systems randomize ~12 bits
  - Brute force can yield results in seconds

INFORMATION LEAKAGE

- Need only discover the location of one library call in an image to offset to the calls you might be interested in

IB-MAC

Separate stacks

- Data stack: contains function arguments, local variables
- Return stack: contains control information
- Can’t use data to overwrite control vectors

Restricted access

- Access to control flow stack restricted
- Only RET and CALL operations are permitted access

Pointer Authentication

ARM v8.3 only

- Hardware defense
- Signs pointer addresses
- Uses unused bits in pointer address space
- Signature checked prior to jump
- Failure leads to program termination

Most 64-bit systems don't use all 64 bits

- Usually about 40 bits
- about 20 available for signing

So how does it work?